UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/538,926	03/30/2000	Vance C. Bjorn	03022.P019	8632

7590 07/28/2004

Judith A Szepesi
Blakely Sokoloff Taylor & Zafman LLP
7th floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	8

DATE MAILED: 07/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.**	**Applicant(s)**
	09/538,926	BJORN ET AL.
	Examiner	**Art Unit**
	Aravind K Moorthy	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-26 are pending in the application.

2. Claims 1-26 have been rejected.

Response to Arguments

3. Applicant's arguments with respect to claims 1-23 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1-4, 6-12 and 22-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Dulude et al U.S. Patent No. 6,310,966 B1.

As to claim 1, Dulude et al discloses a client requesting a cryptographic service. Dulude et al discloses establishing a secure connection between the client and a biometric certification server (BCS). Dulude discloses receiving biometric data from a user. Dulude et al discloses that the BCS performs the cryptographic service if the user is authenticated based on the biometric authentication [column 5 line 50 to column 7 line 25].

As to claims 2 and 25, Dulude et al discloses the cryptographic service is authenticating the user to another server [column 5 line 50 to column 7 line 25].

As to claim 3, Dulude et al discloses generating a temporary public key/private key pair for the user and certifying the public key. Dulude et al discloses forwarding the certificate to the other server [column 5 line 50 to column 7 line 25].

As to claim 4, Dulude et al discloses that the client receives data from the other server for signing with the user's private key. Dulude et al discloses forwarding the data to the BCS. Dulude et al discloses that the BCS signing the data with the user's temporary private key [column 6, lines 13-17].

As to claim 6, Dulude et al discloses detecting an access to a certification database of the client by another server. Dulude et al discloses inserting a temporary certification from the BCS into the certification database of the client. Dulude et al discloses generating a true certificate if the other server chooses the temporary certification [column 5, lines 33-62].

As to claims 7 and 26, Dulude et al discloses that the cryptographic service is signing or encrypting data [column 5, lines 63-67].

As to claim 8, Dulude et al discloses that retrieving a private key/public key pair for the user. Dulude et al discloses performing the cryptographic service with the private or the public key [column 6, lines 1-12].

As to claim 9, Dulude et al discloses detecting an access to a certificate database of the client, as discussed above. Dulude et al discloses detecting the user attempting to perform a cryptographic activity [column 6, lines 28-57].

As to claim 10, Dulude et al discloses receiving a request for a certificate from the server. Dulude et al discloses forwarding the request to a biometric certification server (BCS). Dulude et al discloses receiving a biometric identification from the client and forwarding the biometric identification to the BCS. Dulude et al discloses that if the biometric identification matches a registered user on the BCS, receiving a certificate including a public key of the client certified by the BCS. Dulude et al discloses forwarding the certificate to the server, thereby identifying the client to the server [column 6, lines 50-65].

As to claim 11, Dulude et al discloses detecting an access to a certification database by the server, as discussed above. Dulude et al discloses inserting a temporary certification from the BCS into the certification database, as discussed above. Dulude et al discloses generating a true certificate if the server chooses the temporary certification, as discussed above.

As to claim 12, Dulude et al discloses that the BCS generates a disposable public/private key pair in response to the request. Dulude et al discloses that the BCS certifies the disposable public key of the user [column 7, lines 26-44].

As to claim 22, Dulude et al discloses a crypto-API (application program interface) for receiving cryptographic function requests. Dulude et al discloses a cryptographic service provider for establishing a secure connection to a remote crypto-server. Dulude et al discloses having the crypto-server perform the cryptographic function. Dulude et al discloses a sensor for receiving biometric data from a user. Dulude et al discloses that the biometric data is sent to the crypto-server to authenticate the user and that the remote crypto-server is to perform the requested cryptographic function when the user is successfully authenticated using the biometric data [column 5 line 50 to column 7 line 25].

As to claims 23 and 24, Dulude et al discloses a crypto-API (application program interface) for receiving cryptographic function requests. Dulude et al discloses a cryptographic service provider for establishing a secure connection to a remote crypto-server. Dulude et al discloses having the crypto-server perform the cryptographic function. Dulude et al discloses a sensor for receiving biometric data from a user. Dulude et al discloses that the biometric data sent to the crypto-server to authenticate the user. Dulude et al discloses that the remote crypto-server comprises: a crypto-proxy interface for receiving a request for the cryptographic function from the client on the secure connection; an authentication engine for authenticating the user based on the biometric data; a cryptographic engine for performing the cryptographic functions; and the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed [column 5 line 50 to column 7 line 25].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dulude et al U.S. Patent No. 6,310,966 B1 as applied to claim 1 above, and further in view of Brickell et al U.S. Patent No. 6,310,966 B1.

As to claim 5, Dulude et al does not teach that the client generates a session key for use with the other server. Dulude et al does not teach encrypting the session key with a public key of the other server. Dulude et al does not teach that the client closes the secure connection between the client and the BCS once the session is established between the client and the other server.

Brickell et al teaches that the client generates a session key for use with the other server. Brickell et al teaches encrypting the session key with a public key of the other server [column 8, lines 31-47]. Brickell et al teaches that the client closes the secure connection between the client and the BCS once the session is established between the client and the other server [column 8, lines 31-47].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dulude et al so that the client generated a session key for use with the other server. The session key would have been encrypted with the public key of the other server. The client would have closed the secure connection between the client and the BCS once the session was established between the client and the other server

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dulude et al by the teaching of Brickell et al because the examiner asserts that this prevents a third party from intercepting the session key.

6. Claims 13-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dulude et al U.S. Patent No. 6,310,966 B1 in view of Jakobsson U.S. Patent No. 6,587,946 B1.

As to claim 13, Dulude et al discloses an authentication engine for authenticating the user based on biometric data [column 8, lines 5-50]. Dulude et al discloses a cryptographic engine for performing the cryptographic functions [column 8, lines 5-50].

Dulude et al does not teach a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection. Dulude et al does not teach that the crypto-proxy interface returns data to the client, after the cryptographic functions are performed.

Jakobsson teaches a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection [column 5, lines 48-64]. Jakobsson teaches that the crypto-proxy interface returns data to the client, after the cryptographic functions are performed [column 6, lines 3-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dulude et al so that there would have been a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection. The crypto-proxy interface would have returned the data to the client, after the cryptographic functions was performed.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dulude et al by the teaching of Jakobsson because it is efficient, allows tight control over actions (by the use of quorum cryptography), does not require any pre-computation phase to set up shared keys, and has a trust model appropriate for a variety of settings [column 3, lines 50-58].

As to claim 14, Dulude et al teaches that a database includes user credentials. Dulude et al teaches that the authentication engine retrieving user biometric template from the database and comparing the biometric template to the biometric data received from the user [column 5 line 50 to column 7 line 25].

As to claim 15, Dulude et al teaches a dynamic key generation engine for generating a temporary public key/private key pair, the key pair used for establishing a session between the client and another server, as discussed above.

As to claim 16, Dulude et al teaches the cryptographic engine generating a certificate including the temporary public key, certified by the cryptoserver's private key [column 5 line 50 to column 7 line 25].

As to claim 17, Dulude et al teaches that the dynamic key generation engine destroying the temporary key pair after the session between the client and the other server is successfully established [column 7, lines 26-44].

As to claim 18, Dulude et al suggests a user self-registration interface permitting a user to choose a handle and register a biometric template [column 5 line 50 to column 7 line 25].

As to claim 19, Dulude et al teaches a registration engine for receiving biometric data from the user during a registration process. Dulude teaches extracting the biometric template for the user. Dulude et al teaches a user credential database for storing the handle and the biometric template of the user [column 5, lines 16-49].

As to claim 20, Dulude et al teaches that the registration engine generates a persistent private key/public key pair. Dulude et al teaches a database for storing the persistent private key/public key pair [column 5, lines 16-49].

As to claim 21, Dulude et al teaches a database for storing a persistent private key/public key pair. Dulude et al teaches that the cryptographic engine uses the persistent private key or public key when appropriate to perform the cryptographic functions, as discussed above.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
July 23, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100